National Security Agency/Central Security Service

INFORMATION ASSURANCE DIRECTORATE

CGS Network Security Evaluations Capability

Version 1.1.1

Network Security Evaluations are comprehensive examinations of a network, its architecture, and its defenses. They are used to identify strengths and weaknesses in a given network and provide recommendations for correcting the problems that are identified.

07/30/2012

CGS Network Security Evaluations Capability

Version 1.1.1

Table of Contents

1 Revisions

Name	Date	Reason	Version
CGS Team	30 June 2011	Initial release	1.1
CGS Team	30 July 2012	Inclusion of new IAD document template & Synopsis	1.1.1

2 Capability Definition

The Capability definition provides an understanding of the importance of the Capability to the Enterprise. It provides a high-level overview of the Capability based on definitions derived from Committee on National Security Systems (CNSS) Instruction No. 4009.

Network Security Evaluations are comprehensive examinations of a network, its architecture, and its defenses. They are used to identify strengths and weaknesses in a given network and provide recommendations for correcting the problems that are identified.

Network Security Evaluations are used by Organizations to accomplish several objectives:

- Identify vulnerabilities in operational systems
- Measure the effectiveness of security policy and effect changes
- Demonstrate the impact of network vulnerabilities when attacked

Network Security Evaluations are commonly conducted in two parts, where each part takes a different approach to assessing the network. One approach is to attempt to infiltrate the system by emulating an adversary. The other approach is to conduct the evaluation in cooperation with the local network and system administrators to review the security policies, protections, and network architecture. Network Security Evaluations identify vulnerabilities that exist within a network and provide feedback to the network owners, identifying those vulnerabilities, making recommendations for mitigation, and stating their mission impact.

3 Capability Gold Standard Guidance

The Capability Gold Standard Guidance evaluates the Enterprise needs and overlays the expected Gold Standard behavior. The guidance goes beyond the concept of “good enough” when describing the Gold Standard recommendations, considers industry best practices, and describes a level of security that not only meets current standards but also exceeds them across the Enterprise.

Network Security Evaluations are conducted by the Enterprise as a way to assess their current security posture, identify vulnerabilities, demonstrate the operational impact of an attack, measure the effectiveness of existing security policies, and enumerate the mission impact for each identified vulnerability. The feedback gained from this type of

evaluation shall be used throughout the Enterprise to drive changes to security policies and the security protections employed (as defined in Risk Mitigation).

Although the primary purpose of Network Security Evaluations Capability is not to perform audits or any form of testing for compliance, certification, or accreditation, the results of these evaluations can be useful in support of these activities. Network Security Evaluations shall provide output to other Capabilities, where appropriate, to support these functions (see Enterprise Audit Management, Risk Analysis).

The functions of the Network Security Evaluations Capability can be provided by teams internal to an Enterprise or they can be outsourced to different Organizations. When evaluation teams are maintained internally, they shall be in a separate department from the network and system administrators to prevent conflicts of interest. Internal Network Security Evaluation Teams shall have an ongoing role in network security monitoring. Routine evaluations shall be performed by internal teams if mission needs demand more vigilant security monitoring.

Network Security Evaluation Teams shall comply with any Community-established certification standards. The teams shall consist of individuals who collectively have practical experience covering the wide range of technologies that will be evaluated, information assurance (IA) principles and practices, system and network administration, and an understanding of the hacker's or adversary's mentality and operational methodology.

Network Security Evaluation Teams shall have an official channel through which customers can invite them to conduct their assessment. The individual who commissions the assessment from the customer Enterprise shall have the authority to make and enforce the decision to conduct the evaluation (such as a senior executive or Chief Information Security Officer [CISO]). Having the support of this executive is critical to the success of the evaluation because this person has the authority to request the evaluation, grant access to the team performing the evaluation, and enact changes based on the evaluation findings. Network Security Evaluation Teams report to this senior executive and not to the system administrators for this reason.

At the end of the assessment, the evaluation team shall compile a report, as specified in the scope agreement, which is delivered to the network stakeholders, including system administrators and senior executives. The final report shall highlight the networks that were evaluated, bringing attention to areas of the network or systems that have been

implemented securely and the vulnerabilities that were identified during the evaluation. For each vulnerability, the report also shall provide a mission impact assessment and actionable countermeasures the Enterprise can implement to mitigate the vulnerability.

Network Security Evaluation Teams shall maintain their own test networks for research purposes. Operating a test network allows team members to gather firsthand knowledge of how vulnerabilities affect a network, what implementations work, and which ones do not. From this research, the evaluation team is able to generate realistic best practices and operational details of systems that can be shared with the system administrators of the networks undergoing evaluation.

Network Security Evaluation Teams generally follow either a cooperative or adversarial approach when conducting their assessments, sometimes conducted by what are known as Blue Teams and Red Teams, respectively. The two approaches complement each other because they evaluate the network in different ways. Together, they look at the architecture and security protections in place and identify what has been implemented securely and what needs to be improved upon to better protect the network. Network Security Evaluations taking the cooperative approach are conducted in cooperation with the network's system administrators. Whether the evaluation team is internal to the Enterprise or brought in from the outside, the evaluation team scrutinizes the architecture and implementations on the network, locating vulnerabilities and suggesting remediation activities. Network Security Evaluation Teams taking the adversarial approach play the role of an intruder and attempt to compromise the network in the manner of an attacker to gain insight on the network's security vulnerabilities. Although the senior executive or CISO is aware of the adversarial approach Network Security Evaluation, system administrators shall be unaware that such an evaluation is taking place until after the fact.

The Network Security Evaluation Team and the network being assessed (the customer) shall agree on the rules of engagement and scope of the assessment prior to its start. The evaluation is generally confined to one complete security boundary. This boundary could be a small subnet or an entire Enterprise network, but the scope shall be clearly defined from the beginning. This agreement shall involve legal counsel to ensure all legal provisions are taken into consideration before the evaluation commences.

After an initial scoping meeting with the customer, cooperative approach Network Security Evaluations begin data collection, enumeration, and discovery of as much information about the Enterprise's network and systems as possible. This includes

gathering information from the Enterprise, as well as the team performing scans, to ensure that their knowledge of the network/system architecture is as comprehensive as possible.

The Network Security Evaluation Team performs analysis on the collected data to identify the strengths and weaknesses of the current implementations. Rather than merely identifying symptoms, the team locates the root cause of any problems found. Cooperative approach teams meet daily with the system administrators to disclose any extreme vulnerabilities that were found or quick fixes that can be implemented.

Network Security Evaluation Teams taking the adversarial approach are engaged by their customer to conduct an evaluation initially from outside the Enterprise. They take an adversarial approach and attempt to compromise the network as if they were an attacker. Ideally, the majority of the system administrators on the customer network shall be unaware that the evaluation is going on. Because of this information asymmetry, there shall be a trusted insider who is aware of what is occurring. This individual shall be somewhere in the chain of command such that intrusions will be reported to him or her and he or she can verify whether the activity in question is the result of the evaluation team's actions or an actual intruder.

The adversarial approach Network Security Evaluation Team begins by collecting and analyzing information about the target Enterprise and network. This can include a variety of techniques including, but not limited to, Internet searches and social engineering. Depending on the rules of engagement for the individual exercise, the team may have access to internal resources, if it is mimicking an insider threat. Based on the information collected, the team selects a suitable target for attack. This target may or may not be the final goal of the intrusion; it is the first step into the network. The team analyzes the target for vulnerabilities and plans how to gain access.

After establishing the target, the team gains a foothold on the network by gaining access to that target. If this initial target system is outside the scope of the customer's control, additional permission shall be obtained from the target's owner. Access to the target machine is usually secured by gaining administrative access to the system. At this point, the evaluation team uses software and other tools to maintain its access. From the target, the team expands its access by exploiting trust relationships between the initial target and other systems on the network. At each new system, the team repeats the process of collecting information, selecting a target, gaining a foothold, securing access, expanding access, and then collecting information again.

Network Security Evaluations are not the same as penetration tests. Penetration testing is used to identify security holes and test network defenses. They can be noisy and can be performed with the purpose of being detected and generating a response from the defenders. Penetration testing does not evaluate mission impact. Network Security Evaluation Teams may use penetration testing as a component of their evaluations.

Part of the analysis conducted by Network Security Evaluations is to identify evidence of unauthorized activity on the network. Unauthorized activity can be the result of attackers infiltrating the network or from unintentional or malicious insider activity. If any unauthorized activity is identified that represents a threat to the network being evaluated, the team performing the evaluation will alert the network owners immediately and, depending on the rules of engagement, immediately stop evaluation activities. The information uncovered about unauthorized activity will feed into the Incident Response capability.

Network Security Evaluations accumulate a lot of data about a network over the course of their evaluations. This data shall be removed from the network as soon as feasible to prevent being compromised by an intruder. The data shall be handled with the utmost care, protected by strong encryption, and securely destroyed following the engagement.

Network Security Evaluations use a diverse set of tools while conducting their evaluations. Some of the tools may be publically available and others are highly specialized, custom-made tools. All tools shall be vetted and approved in accordance with established standards. In addition, all tools shall be uniquely identifiable by the team using them so they can be distinguished from tools used by unauthorized intruders. All tools shall be protected to prevent their unauthorized disclosure or use. Some of the protection techniques include encryption, secure deletion, and runtime protection. To further prevent unauthorized use, tools used for penetration (adversarial) purposes may be specifically designed so they are not intuitive to use and lack help functions. If tools are going to be left behind for use by the customer or the Network Security Evaluation Team as part of a follow-on or future assessment, they need to be thoroughly documented. Custom tools shall be resistant to reverse engineering and never use undocumented exploits.

After conducting a Network Security Evaluation, the evaluation team shall make non-attributable findings from their evaluation available to other members of the Community. This will allow for statistical analysis and trending as well as greater awareness of

security vulnerabilities. It is imperative that these findings be non-attributable so they cannot be associated with the Enterprise from which they were generated.

4 Environment Pre-Conditions

The environment pre-conditions provide insight into environmental, user, and technological aspects needed for Capability implementation. These pre-conditions are services or other Capabilities that must be in place within the Enterprise for the Capability to function.

1. All legal procedures are defined to provide authority to the evaluation teams prior to testing.
2. A stable network environment exists.
3. Executive buy-in has been obtained to ensure mitigations provided by the evaluation will be incorporated within the network.
4. The customer has defined a cooperative trusted agent.
5. There is an IA staff that is independent from the Information Technology staff.
6. The mission is understood.

5 Capability Post-Conditions

The Capability post-conditions define what the Capability will provide. They define functions that the Capability will perform or constraints that the Capability will operate under when performing its function.

1. The Capability provides a report of the activities of the evaluation.
2. The Capability does not perform auditing or compliance certification.
3. The Capability may not find/document all vulnerabilities within the network.
4. The Capability provides the recommended mitigations, but the owner or system/network administrators are ultimately responsible for implementation.
5. The results provided by this Capability can feed into certification and accreditation decisions.
6. The Capability provides certified, trained individuals.

6 Organizational Implementation Considerations

Organizational implementation considerations provide insight into what the Organization needs to establish, ensure, and have in place for the specified Capability to be effective. It provides guidance specific to the actions, people, processes, and departments that an Organization will need to execute or establish to implement the guidance described in Section 3 (Capability Gold Standard Guidance).

The Organization will determine whether it is more efficient for it to maintain this Capability internally or to outsource its functions. The advantages to maintaining these teams internally include greater flexibility in conducting evaluations and defining scope, increased involvement by the team in fixing vulnerabilities, and ongoing monitoring. The Organization will make this decision based on the needs of the missions it supports. For those Organizations that provide this Capability internally, Network Security Evaluation Teams will have an ongoing role in keeping the network secure. The department performing these IA tasks will be separate from the system and network administrators. System administration and IA are demanding tasks that have to balance what are sometimes competing needs, and having both tasks assigned to the same department could result in a conflict of interest.

The Organization may choose to use Network Security Evaluations under a number of circumstances and will have internally established policies governing their use. These policies will be developed and maintained by a department separate from the system and network administrators. Generally, the Organization will have these evaluations performed on an event-driven basis as opposed to a time-driven basis. However, depending on mission criticality and Organization policy, evaluations may be conducted based on time as well. At a minimum, an Organization will have Network Security Evaluations conducted every 2 years. Some of the events that may prompt an Organization to initiate an evaluation include the following:

- After experiencing an IA incident
- After experiencing a network intrusion
- As part of a certification and accreditation process
- When deploying new technology
- When implementing new security policies
- To determine the mission impact of a security breach
- As part of an exercise

One of the requirements for performing a Network Security Evaluation is a stable network. The Organization can have evaluations conducted on operational networks or networks that have not been transitioned to operational use. If an evaluation is conducted on a network not yet in operational use, it will accurately reflect all of the configurations that it will have when put into operation. Either way, the network being evaluated will be stable and not undergoing any functional changes at the time of the evaluation or soon afterward. Performing an evaluation on an unstable network may cause inconsistencies in the results and indications of false positives.

When conducting a cooperative approach Network Security Evaluation, the Organization will ensure that all network and system administrators cooperate with the evaluation team's efforts. Cooperative information sharing will allow the team to do its job more effectively and provide the best possible results.

When conducting an adversarial approach Network Security Evaluation, the trusted insider working with the evaluation team will ensure that all proper reporting policies are being followed to prevent triggering unnecessary emergency response procedures (see Incident Response). Maintaining limited knowledge by the trusted insider of the ongoing evaluation will be important because it will prevent artificially bolstered network defense and monitoring.

Following a Network Security Evaluation, the Organization will review the report containing the evaluation's findings and recommendations. Because Network Security Evaluations do not conduct any form of certification or accreditation, the Organization will be responsible for deciding which recommendations to implement within its Enterprise. The Organization will have to make this decision based on the mission and financial impact of each recommendation, and based on the overall risk tolerance of the Organization (see Risk Analysis).

The Organization will use the non-attributable findings from the Network Security Evaluations of other members of the Community to assess its network security posture. These findings will feed into the Organization's Vulnerability Assessment Capability.

7 Capability Interrelationships

Capability interrelationships identify other Capabilities within the Community Gold Standard framework that the Capability in this document relies on to operate. Although there are many relationships between the Capabilities, the focus is on the primary relationships in which the Capabilities directly communicate with or influence one another.

7.1 Required Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are necessary for the Capability in this document to operate.

- Vulnerability Assessment–The Network Security Evaluations Capability relies on the Vulnerability Assessment Capability to provide information on emerging vulnerabilities so that testing techniques can be adjusted.

7.2 Core Interrelationships

The following Capability interrelationships include the Capabilities within the Community Gold Standard framework that relate to every Capability.

- Portfolio Management–The Network Security Evaluations Capability relies on the Portfolio Management Capability to determine current and future investment needs and prioritize investments based on those needs.
- IA Policies, Procedures, and Standards–The Network Security Evaluations Capability relies on the IA Policies, Procedures, and Standards Capability to provide information about applicable federal laws, Executive Orders, regulations, directives, policies, procedures, and standards.
- IA Awareness–The Network Security Evaluations Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.
- IA Training–The Network Security Evaluations Capability relies on the IA Training Capability to provide training programs related to IA activities in accordance with agency policies.
- Organizations and Authorities–The Network Security Evaluations Capability relies on the Organizations and Authorities Capability to establish the relevant roles and responsibilities.

7.3 Supporting Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are not necessary for the Capability to operate, although they support the operation of the Capability in this document.

- Network Mapping–The Network Security Evaluations Capability relies on the Network Mapping Capability to provide information to evaluations teams.
- Network Boundary and Interfaces–The Network Security Evaluations Capability relies on the Network Boundary and Interfaces Capability to provide information to evaluations teams.
- Utilization and Performance Management–The Network Security Evaluations Capability relies on the Utilization and Performance Management Capability to provide information to evaluations teams.
- Understand Mission Flows–The Network Security Evaluations Capability relies on the Understand Mission Flows Capability to provide information to evaluations teams.
- Understand Data Flows–The Network Security Evaluations Capability relies on the Understand Data Flows Capability to provide information to evaluations teams.

- Hardware Device Inventory–The Network Security Evaluations Capability relies on the Hardware Device Inventory Capability to provide information to evaluations teams.
- Software Inventory–The Network Security Evaluations Capability relies on the Software Inventory Capability to provide information to evaluations teams.
- Understand the Physical Environment–The Network Security Evaluations Capability relies on the Understand the Physical Environment Capability to provide information to evaluations teams.
- Network Enterprise Monitoring–The Network Security Evaluations Capability relies on the Network Enterprise Monitoring Capability to provide information as a component of its data gathering process.
- Network Hunting–The Network Security Evaluations Capability relies on the Network Hunting Capability to provide information about previously unknown vulnerabilities to incorporate into assessment methods.
- Enterprise Audit Management–The Network Security Evaluations Capability relies on the Enterprise Audit Management Capability to provide audit logs as a part of its data collection process.

8 Security Controls

This section provides a mapping of the Capability to the appropriate controls. The controls and their enhancements are granularly mapped according to their applicability. In some instances, a control may map to multiple Capabilities.

Control Number/Title	Related Text
NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*	
CA-2 *SECURITY ASSESSMENTS*	Control: The organization: a. Develops a security assessment plan that describes the scope of the assessment including: Security controls and control enhancements under assessment; Assessment procedures to be used to determine security control effectiveness; and Assessment environment, assessment team, and assessment roles and responsibilities;

	b. Assesses the security controls in the information system [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system; c. Produces a security assessment report that documents the results of the assessment; and d. Provides the results of the security control assessment, in writing, to the authorizing official or authorizing official designated representative. Enhancement/s: (1) The organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the information system. (2) The organization includes as part of security control assessments, [Assignment: organization-defined frequency], [Selection: announced; unannounced], [Selection: in-depth monitoring; malicious user testing; penetration testing; red team exercises; [Assignment: organization-defined other forms of security testing]].
SA-12 *SUPPLY CHAIN PROTECTION*	Enhancement/s: (7) The organization employs independent analysis and penetration testing against delivered information systems, information system components, and information technology products.
SA-31 *COVERT CHANNEL ANALYSIS*	Control: The organization requires that information system developers/integrators perform a covert channel analysis to identify those aspects of system communication that are potential avenues for covert storage and timing channels. Enhancement/s: (1) The organization tests a subset of the vendor-identified covert channel avenues to determine if they are exploitable.

9 Directives, Policies, and Standards

This section identifies existing federal laws, Executive Orders, regulations, directives, policies, and standards applicable to the Capability but does not include those that are agency specific.

Network Security Evaluations Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
Nothing found	
Comprehensive National Cybersecurity Initiative (CNCI)	
NSPD-54/HSPD-23 Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]), 8 January 2008, Classified	Summary: National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-54/HSPD-23), in which the Comprehensive National Cybersecurity Initiative (CNCI) is described, is classified. Initiative 7 deals with increasing the security of classified networks.
Department of Defense (DoD)	
DoDD 8500.01E Summary: Information Assurance (IA), 23 April 2007, Unclassified	This directive establishes policy and responsibility related to information assurance (IA) readiness throughout all Department of Defense (DoD) components. Red and Blue teams are part of IA readiness.
DoDI O-8530.1 Computer Network Defense (CND), 8 January 2001, Classified	Summary: This directive states that an effective Computer Network Defense (CND) is predicated upon robust infrastructure and IA practices, including regular and proactive vulnerability analysis and assessment, and implementation of identified improvements.
DoDI 8560.01 Communications Security (COMSEC) Monitoring and Information Readiness Testing (IA Readiness Testing), 9 October 2007, Unclassified	Summary: This instruction established and implements DoD policies and responsibilities for conducting IA readiness testing, which is defined to include Red Team efforts.
CJCSI 6510.01E,	Summary: This instruction assigns responsibilities for IA

Information Assurance (IA) and Computer Network Defense (CND), 12 August 2008, Unclassified	and CND activities across the DoD components.
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, …)	
Nothing found	
Executive Branch (EO, PD, NSD, HSPD, …)	
Nothing found	
Legislative	
Nothing found	

Network Security Evaluations Standards

Title, Date, Status	**Excerpt / Summary**
Intelligence Community (IC)	
Nothing found	
Comprehensive National Cybersecurity Initiative (CNCI)	
Nothing found	
Department of Defense (DoD)	
Nothing found	
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, …)	
Nothing found	

Executive Branch (EO, PD, NSD, HSPD, …)	
Nothing found	
Legislative	
Nothing found	
Other Standards Bodies (ISO, ANSI, IEEE, …)	
Nothing found	

10 Cost Considerations

This section provides examples of some of the types of costs that the Organization will need to consider when implementing this Capability. The following examples are costs that are common across all of the Community Gold Standards Capabilities:

1. Solution used for implementation (hardware and/or software)
2. Necessary training
3. Licensing (if applicable)
4. Lifecycle maintenance
5. Impact/dependency on existing services
6. Manpower to implement, maintain, and execute
7. Time to implement, maintain, and execute
8. Network bandwidth availability and consumption
9. Scalability of the solution relative to the Enterprise
10. Storage and processing requirements

In addition to the common costs, the following are examples of cost considerations that are specific to this Capability:

1. Solution used for implementation–The Enterprise will need to provide the requisite tools and equipment (hardware and software) for this Capability.
2. Manpower to implement, maintain, and execute–If the Capability is maintained internal to the Enterprise rather than being outsourced, it will require dedicated personnel. Evaluations may require travel. Specialized tools may need to be developed. Mitigations must be researched and tested. Legal oversight is required for all evaluations.
3. Time to implement, maintain, and execute–Evaluation process and preparation can be time-consuming.

11 Guidance Statements

This section provides Guidance Statements, which have been extracted from Section 3 (Capability Gold Standard Guidance) of this Capability document. The Guidance Statements are intended to provide an Organization with a list of standalone statements that are representative of the narrative guidance provided in Section 3. Below are the Guidance Statements for the Network Security Evaluations Capability.

- The Enterprise shall conduct evaluations of network security as a way to assess their current security posture, identify vulnerabilities, demonstrate the operational impact of an attack, measure the effectiveness of existing security policies, and enumerate the mission impact for each identified vulnerability.
- Feedback gained from network security evaluations shall be used throughout the Enterprise to drive changes to security policies and the security protections employed.
- Network security evaluations shall be performed by internal teams if mission needs demand more vigilant security monitoring.
- When network security evaluation teams are maintained internally, they shall be in a separate department from the network and system administrators to prevent conflicts of interest.
- Internal network security evaluation teams shall have an ongoing role in network security monitoring.
- Network security evaluation teams shall comply with any Community-established certification standards.
- Network security evaluation teams shall consist of individuals who collectively have practical experience covering the wide range of technologies that will be evaluated, IA principles and practices, and system and network administration, and an understanding of the hacker or adversary's mentality and operational methodology.
- Network security evaluation teams shall have an official channel through which customers can invite them to conduct their assessment.
- The individual who commissions the assessment from the customer Enterprise shall have the authority to make and enforce the decision to conduct the evaluation (such as a senior executive or CISO).
- The network security evaluation teams shall compile a report at the end of an assessment, which is delivered to the network stakeholders. The final report shall highlight the networks that were evaluated, the areas of the network or systems that have been implemented securely, and the identified vulnerabilities.

- The network security evaluation report shall provide a mission impact assessment and actionable, implementable countermeasures for each identified vulnerability.
- Network security evaluation teams shall maintain their own test networks for research purposes to allow team members to gather firsthand knowledge of how vulnerabilities affect a network, which implementations work, and which ones do not.
- The network security evaluation teams and the network being assessed (its customer) shall agree on the rules of engagement and scope of the assessment prior to its start. This agreement shall involve legal counsel to ensure all legal provisions are taken into consideration before the evaluation commences.
- Network security evaluations shall include data collection, enumeration, and discovery of as much information about the Enterprise's network and systems as possible. This includes gathering information from the Enterprise, as well as the team performing scans, to ensure that their knowledge of the network/system architecture is as comprehensive as possible.
- The network security evaluation team shall perform analysis on collected data to identify the strengths and weaknesses of the current implementations and identify the root cause of any problems found.
- When a network security evaluation team conducts an evaluation from outside the Enterprise, the majority of the system administrators on the customer network shall be unaware that the evaluation is occurring, and there shall be a trusted insider who is aware that it is occurring.
- The network security evaluation team shall select a suitable target for attack based on the information collected about the target Enterprise and network.
- The network security evaluation team shall analyze the established target for vulnerabilities and plan how to gain access.
- The network security evaluation team shall attempt to gain a foothold, secure access, and expand access for each new established target.
- Network security evaluations shall identify evidence of unauthorized activity on the network. If any unauthorized activity is identified that represents a threat to the network being evaluated, the team performing the evaluation shall alert the network owners immediately and, depending on the rules of engagement, immediately stop evaluation activities.
- Data accumulated from network security evaluations shall be removed from the network as soon as feasible to prevent compromise by an intruder. The data shall be handled with the utmost care, protected by strong encryption, and securely destroyed following the engagement.

- All network security evaluation tools shall be vetted and approved in accordance with established standards.
- All network security evaluation tools shall be uniquely identifiable by the team using them so they can be distinguished from tools used by unauthorized intruders.
- All network security evaluation tools shall be protected to prevent their unauthorized disclosure or use by techniques such as encryption, secure deletion, and runtime protection.
- Custom tools shall be resistant to reverse engineering and shall never use undocumented exploits.
- Tools left behind for customer use following the assessment shall be thoroughly documented and shall be resistant to reverse engineering.
- After conducting a network security evaluation, the evaluation team shall make non-attributable findings from their evaluation available to other members of the Community to allow for statistical analysis and trending as well as greater awareness of security vulnerabilities.